Wireless at Iowa State

ISU
Wireless Communication Systems

Presented to: Telcordia™ Technologies — *Performance from Experience*

by

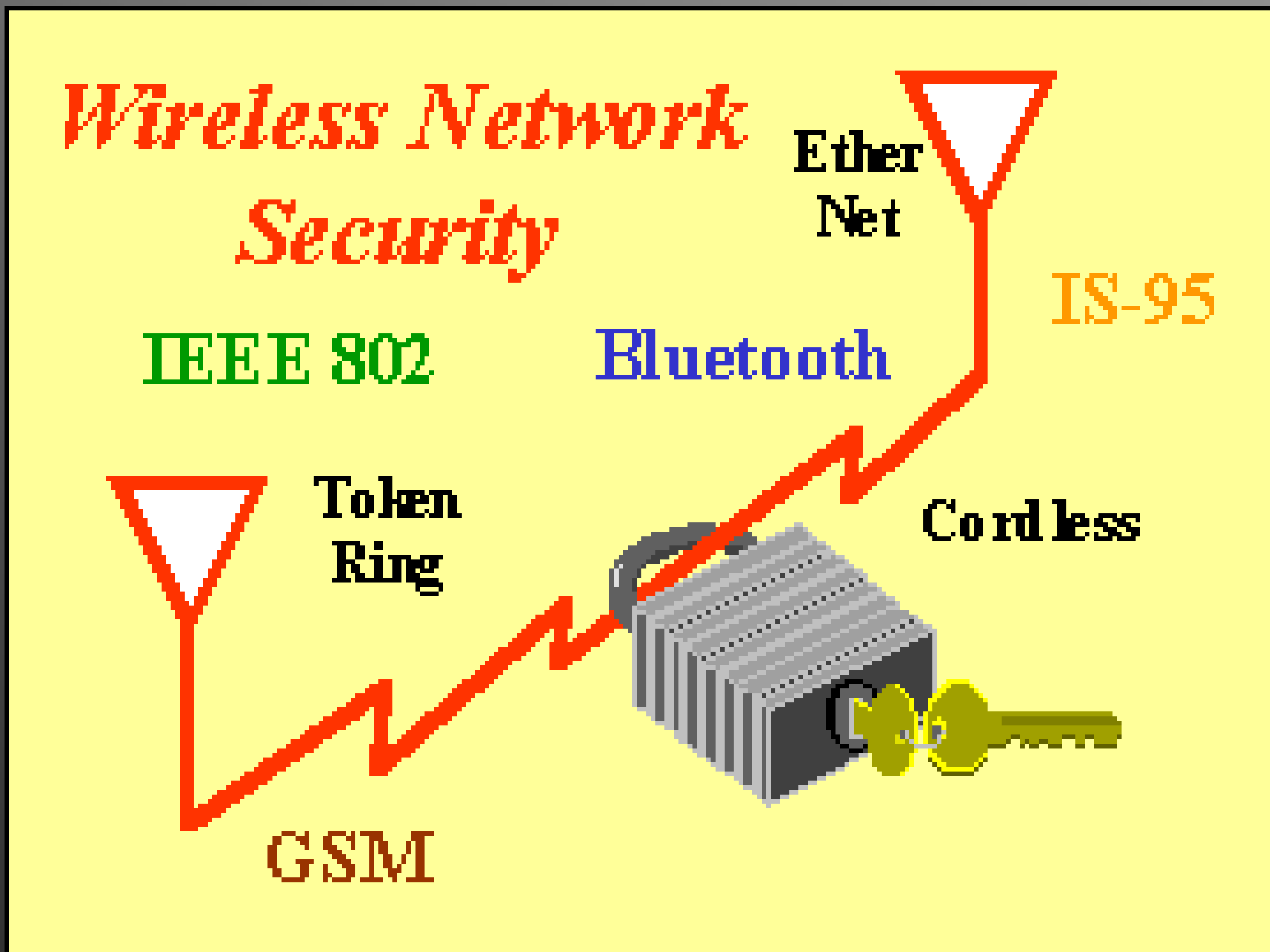
Steve F. Russell

Iowa State University

Department of Electrical and Computer Engineering

August 17, 2000

WIRELESS
COMMUNICATION
SYSTEMS



1

Summer 2000

Motivation

Speech by Secretary of Defense William S. Cohen, February 18, 1999

- ***There is a sense ... that some in the "digital world" dismiss the importance of the national security world.***
- ***We are ...preparing for the future by addressing dangers you know well -- threats to the integrity of our information infrastructure.***
- ***Today, as you well know, small groups, even single individuals, can wage electronic war against the most powerful nation in the world using off the shelf, existing tools and technologies.***
- ***All together, the Department of Defense will spend $3.6 billion on computer security in the next four years.***

http://www.defenselink.mil/speeches/1999/s19990218-secdef.html

2

Changing Needs

ISU
Wireless Communication Systems

- The public need for wireless reliability and privacy increased dramatically when PCS started to become a reality
- In the past, reliability and privacy issues were addressed from the viewpoint of the service provider -- not necessarily the user
- Future systems must satisfy the needs of users as well

3

Need for Wireless Security

ISU
Wireless Communication Systems

- Wireless communication systems are very vulnerable to denial-of-service attacks
- Wireless network links are natural “wire taps” into a network
- Users are generally unaware of the security issues associated with a wireless link
- “End-to-end’ seamless security needs to be provided by the equipment manufacturers

4

Principal Investigator Background

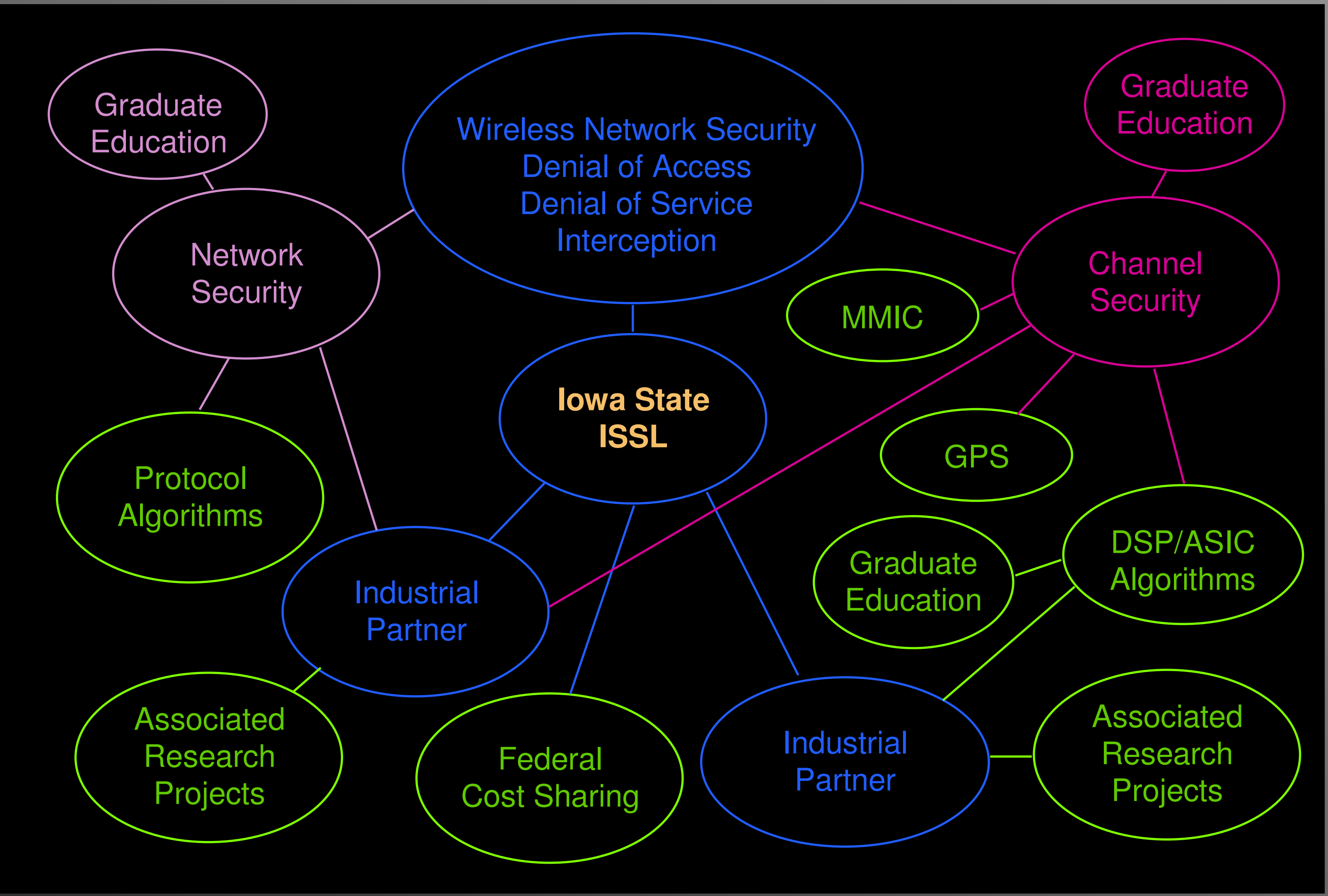
ISU
WIRELESS
COMMUNICATION
SYSTEMS

- Rockwell-Collins, GPS Programs, High Anti-jam General Development Model (GDM), 4 years
- Anti-jam receiver design at Rockwell
- Author of anti-jam systems design monograph at Rockwell
- Consultant to RCA/Camden on high-antijam frequency-hopping communication system
- PI on wireless security grant from Rockwell Foundation, 2 years
- Developed wireless security program and web site at ISU

5

Cooperative Learning/Research

ISU
Wireless Communication Systems



6

Wireless Network Security Research and Education at ISU

ISU
WIRELESS
COMMUNICATION
SYSTEMS

- Unique program started by ISU
- Startup supported by a grant from the Rockwell
- Collaboration with Information Systems Security Group, ISSL Lab
- Research focus is physical (and network) layer design, intrusion detection, and counterfeit base
- New graduate course, CPrE 537 in Wireless Communications Security
    - First in the country

7

Information Systems Security

WIRELESS
COMMUNICATION
SYSTEMS

- Information (Data) Security
- Computer Security
- Network Security
- Wireless Channel Security

8

Security Services Provided by a Telecommunication System

WIRELESS COMMUNICATION SYSTEMS

- Identification and Authentication
- Privacy
- Reliability

9

Electronic Warfare

SERVICE	ECM	ECCM
Authentication	Spoofing	Anti-Spoofing
Privacy	Intercept	Anti-Intercept
Reliability	Jam	Anti-Jam

10

Security and Reliability Issues and Perceptions

ISU
Wireless Communication Systems

- The Service Provider
- The Equipment Manufacturer
- The Customer

11

The Service Provider

ISU
WIRELESS
COMMUNICATION
SYSTEMS

- Loss of Revenue
- Quality of Service
- Customer Perceptions

12

The Equipment Manufacturer

WIRELESS COMMUNICATION SYSTEMS

- Cost
- Reliability
- Customer and Service Provider Perceptions

13

The Customer

- Cost
- Reliability
  - Robust Airlink
  - Antijam and Anti-interference
- Privacy (Security and anonymity)
  - Encryption
  - Position Location and Identification (E 9-1-1)
  - User identification outside the service providers system

Examples of Lost Privacy

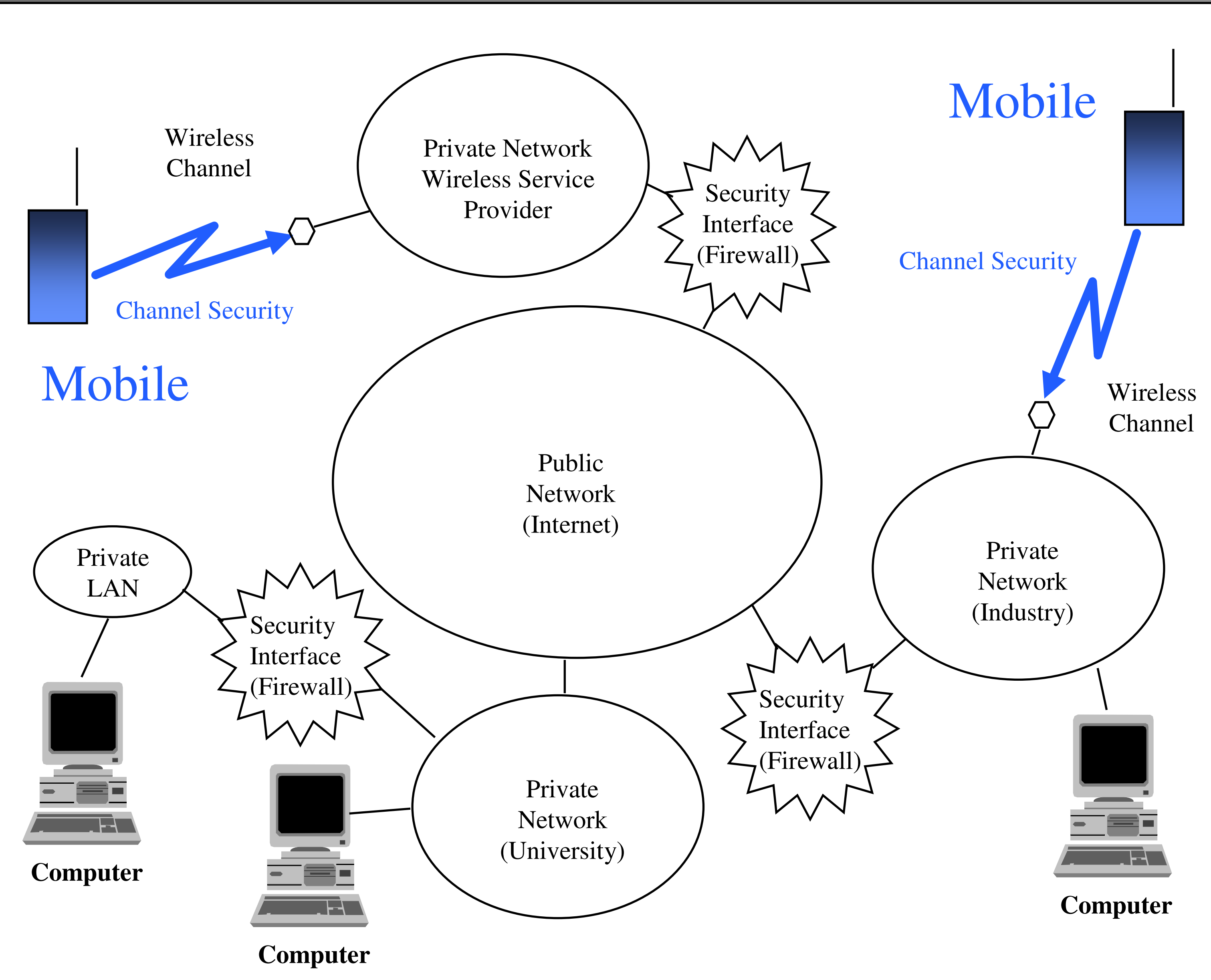
- Wireless Enhanced 9-1-1*
  - Implemented by October 2001
  - Location of Mobile Station Must be Provided to Public Safety Answering Point
  - Latitude & Longitude
    - Accuracy of 125 Meters 67% of the Time
  - Users need to be able to deny this capability or only enable for actual 9-1-1 calls
- Transmitter waveform signature identification ("Transmitter Fingerprinting")

15

*Based on a presentation by Betsy Kidwell
Wireless Standards Development, Lucent Technologies
National Communications Forum 1997

Some Wireless Systems

- Cellular Radio Telephone
  - FDMA (AMPS, Analog FM)
  - TDMA (D-AMPS, GSM)
  - CDMA (IS-95)
- Wireless LAN
  - 802-11
  - Bluetooth
  - etc. etc.
- Land Mobil and Special Mobile Radio (SMR)
- Cordless Telephone



ISU
WIRELESS
COMMUNICATION
SYSTEMS

Secure Wireless Communications

17

Some Security Issues

ISU
WIRELESS
COMMUNICATION
SYSTEMS

- Encryption
- Interception
- Jamming or Service Degradation (Intentional)
- Interference (unintentional)
- Position Location

18

Electronic Security Model for Civil Systems

ISU
Wireless Communication Systems

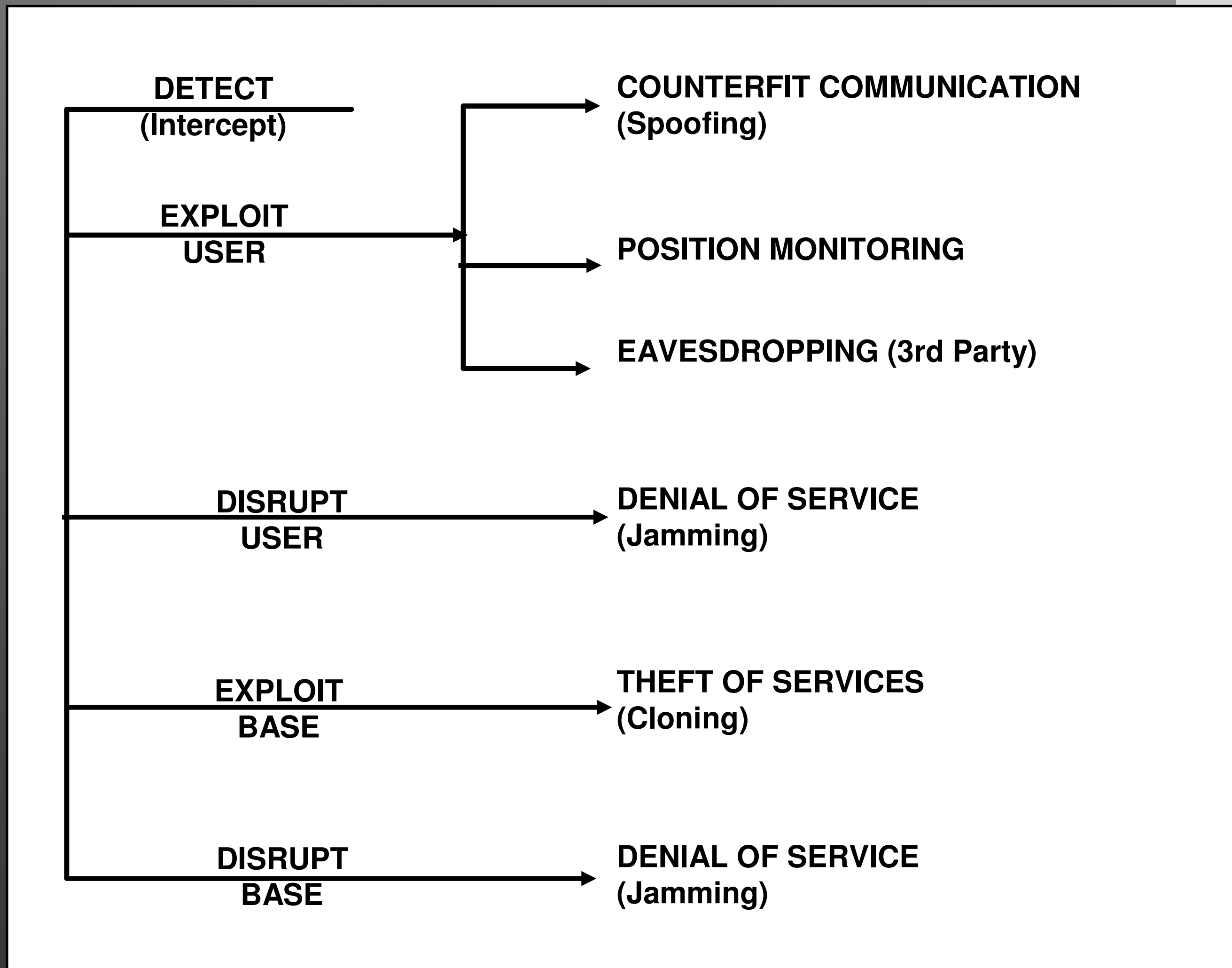


Fig. 0085

19

Past, Immediate and Future Threats

ISU
Wireless Communication Systems

- **Number Cloning**
  - Skills and technology costs needed to clone numbers are relatively low
  - This was a significant problem for service providers in the past but effective solutions are now available
- **Decryption**
  - Computational time and costs are prohibitive for advanced methods
  - Encryption techniques continue to advance to the point where this is not a problem in well-designed systems

Past, Immediate and Future Threats (cont.)

- **Intrusion**
  - This is a significant threat but is still too costly and/or sophisticated except for government agencies
  - Intrusion detection methods are still in the research stage and much work remains to be done
  - IS-95 counterfeit base (an example is given later)
- **Position Location**
  - The technologies being developed for E911 can be used for locating and tracking individuals
  - Public resistance to “big brother” tracking will increase

Immediate and Future Threats (cont.)

WIRELESS COMMUNICATION SYSTEMS

- Denial-of-Service
  - Antijam system designs are needed
  - Data Interleaving and proper media access control (MAC) design can improve reliability
- Spoofing
  - System designs must improve the ways that both the mobile and base are identified and authenticated

The simple, low-cost strategies

ISU
WIRELESS
COMMUNICATION
SYSTEMS

- Denial-of-Service (DOS)
  - Brute force jamming (barrage jamming)
    - “Wavewall” product (Demo?)
  - Base station call setup spoofing
  - False control signals over the setup (usually paging) channel
- Eavesdropping
  - Forced analog operation (jam the TDMA or CDMA cellphone channel
  - Base station impersonation (very costly in some systems but easy in some cordless phones)

ISU
Wireless Communication Systems

A well-designed denial-of-service attack will act like network congestion or an intermittent data connection

24

Wireless Channel Security
"The Big Tradeoff"

ISU
Wireless
Communication
Systems

Reliability
&
Privacy

Data
Throughput

ISU
Wireless Communication Systems

❖ Modeling

Wireless Network Model

Simplified Diagram of a Wireless Access Point in a Wireless Local Area Network

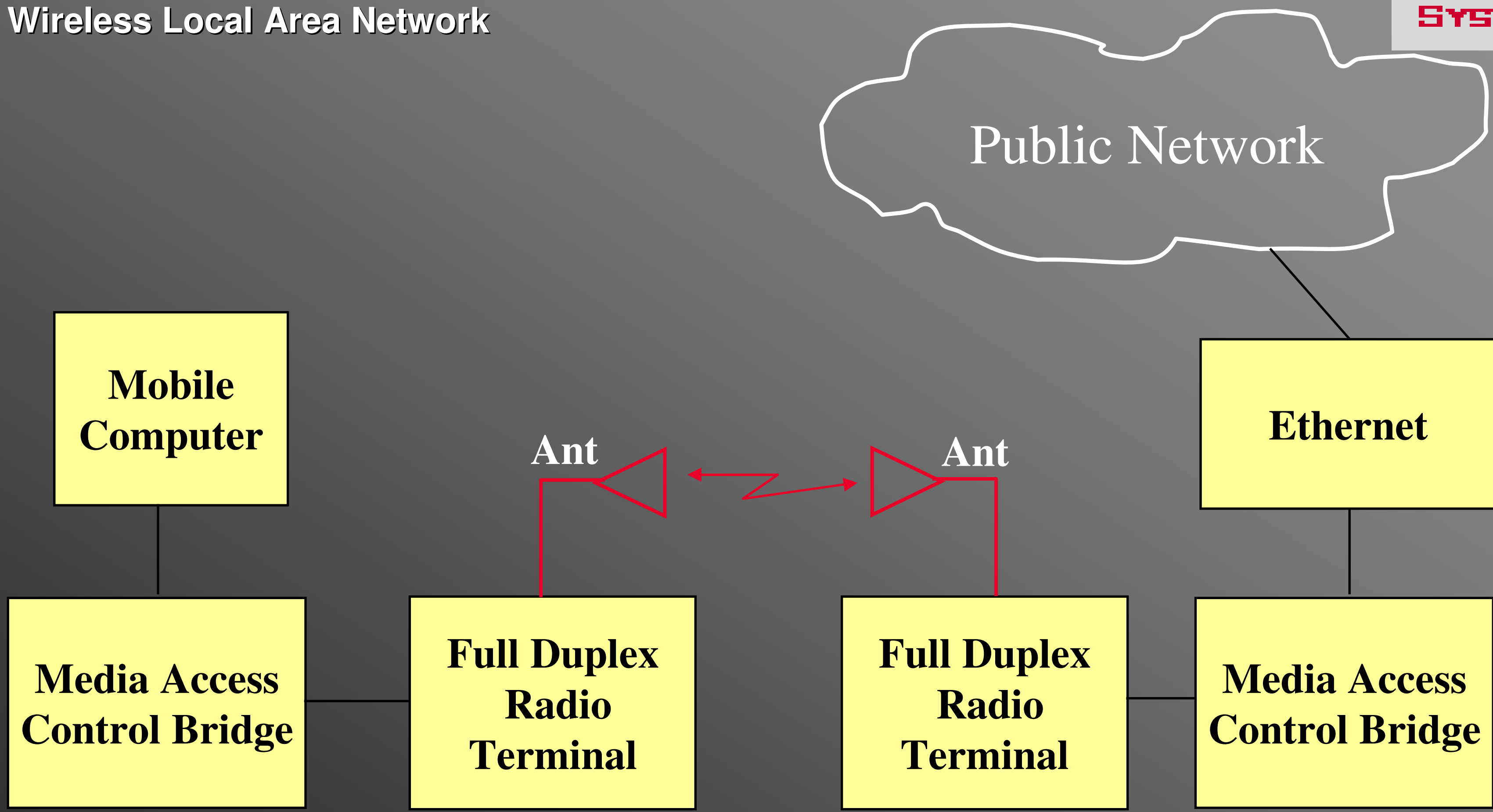
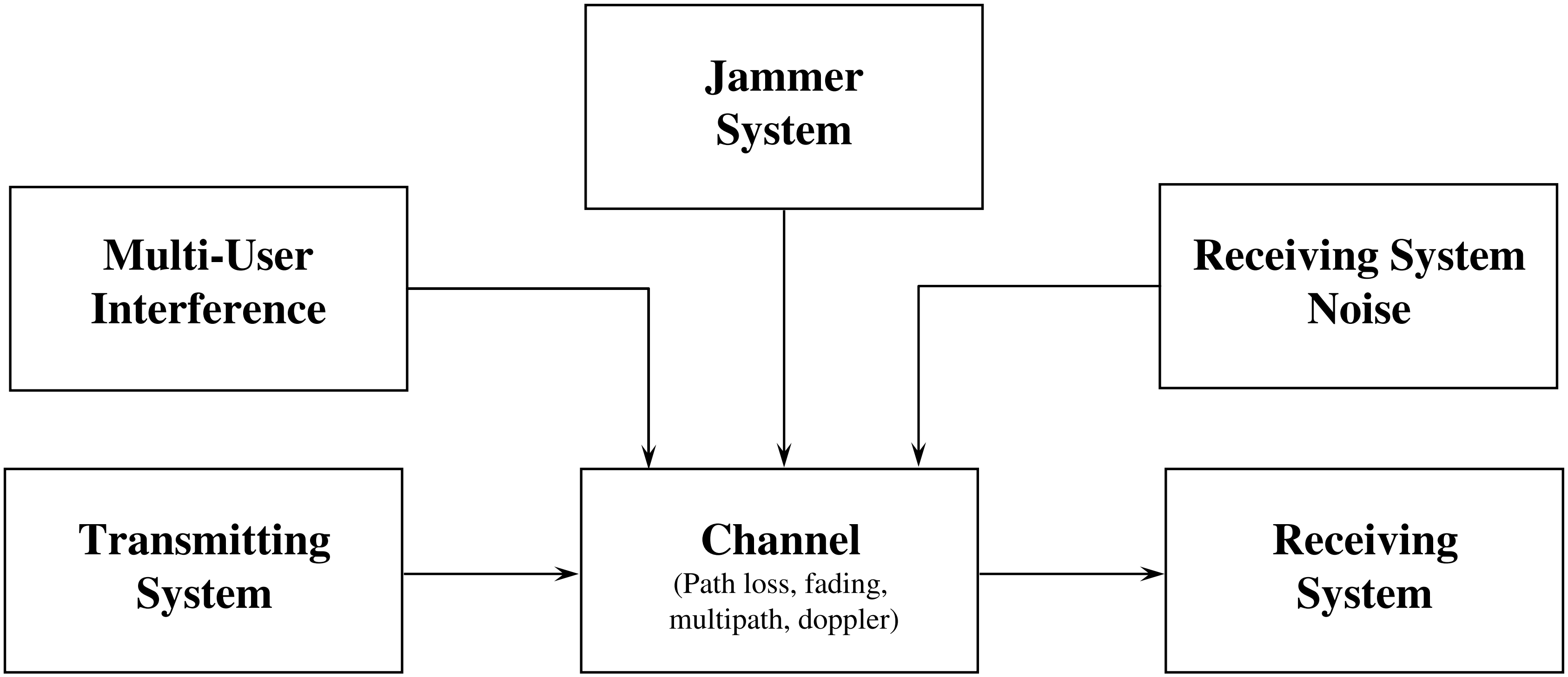


Fig. 0150

27



Basic System Components in a Multi-User, Spread-Spectrum Communication System

Fig. 0002

28

Wireless Channel Security Scenario

ISU
WIRELESS
COMMUNICATION
SYSTEMS

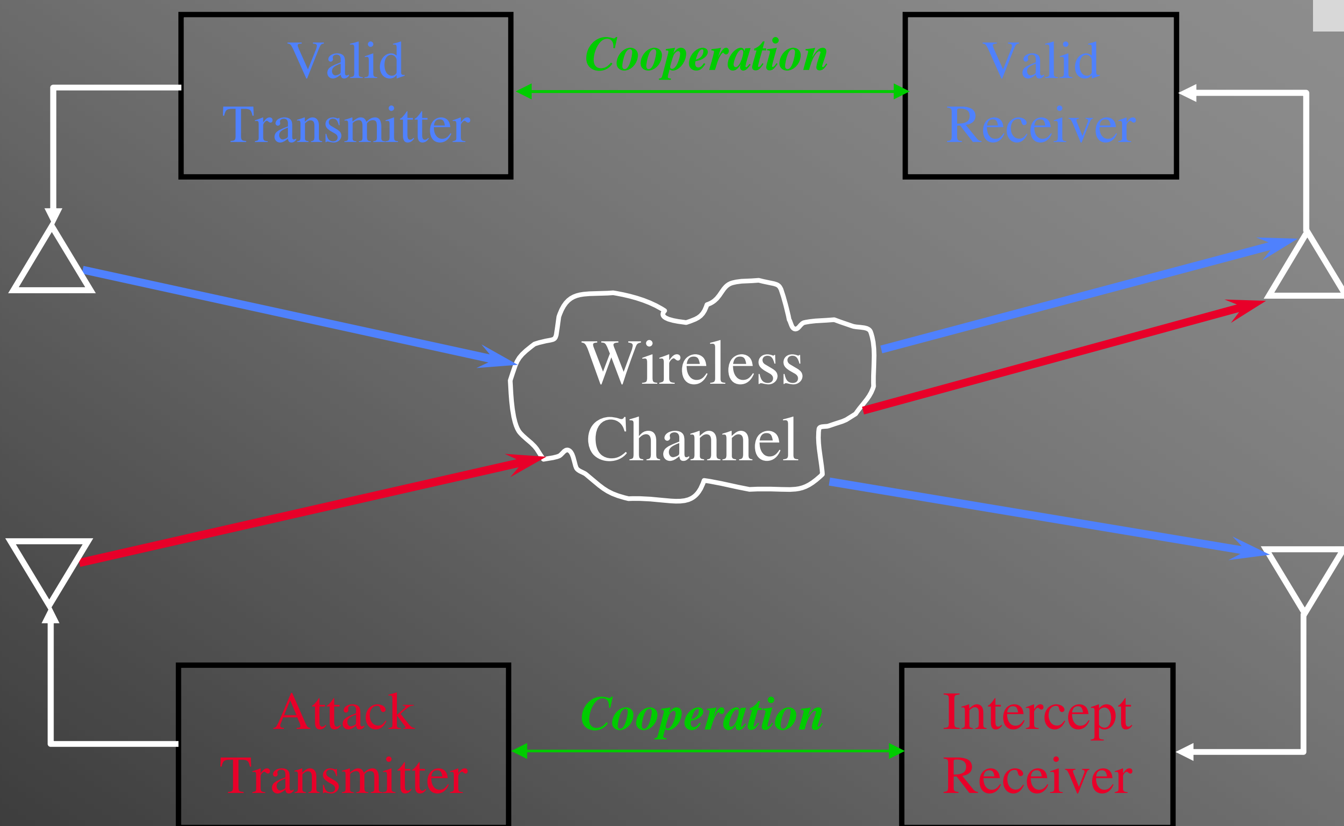
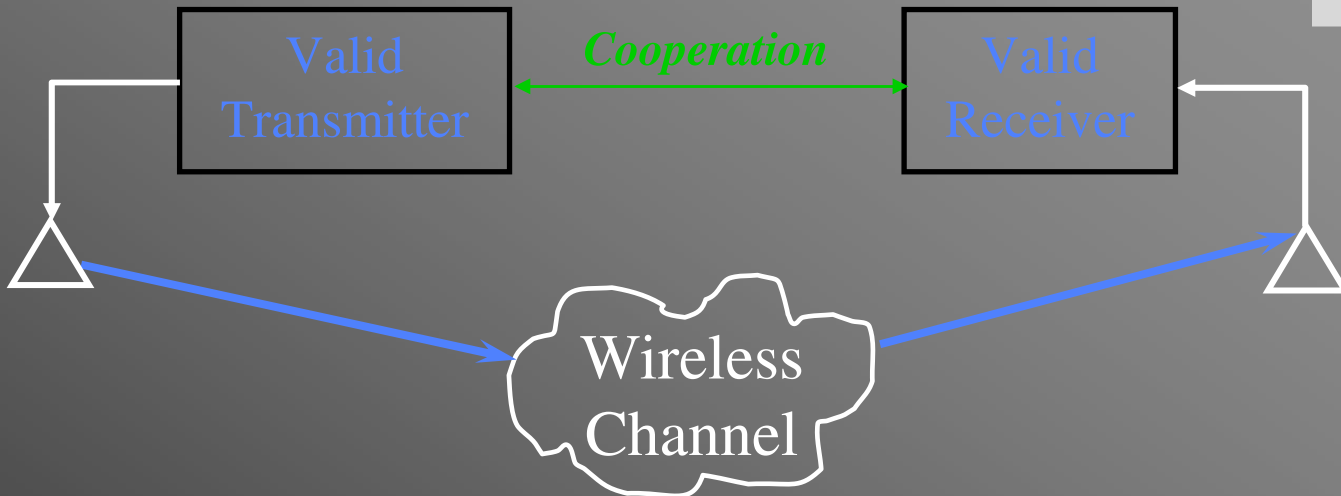


Fig. 0146

Normal Operation



30

Eavesdropping Scenario

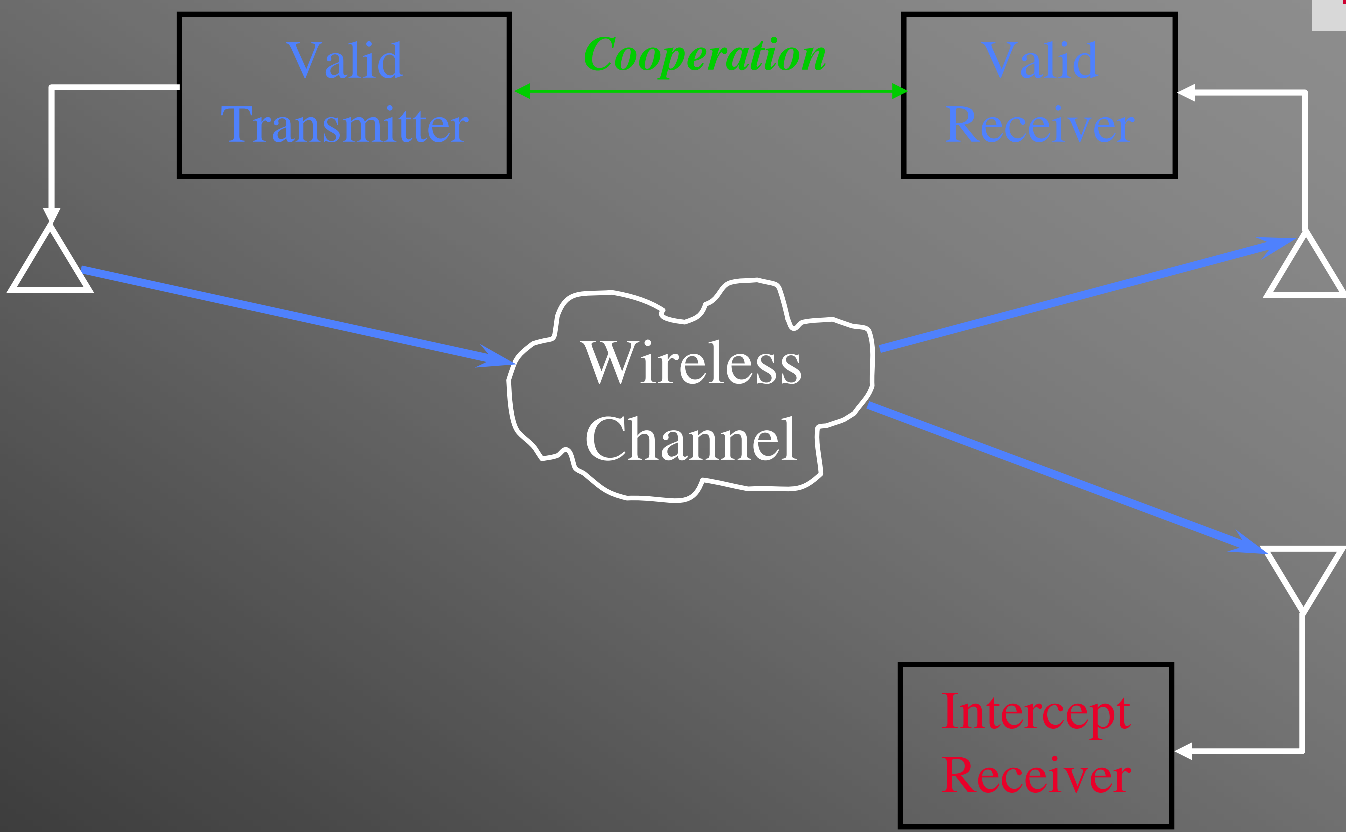


Fig. 0146

31

Jamming Scenario
(Denial-of-Service Attack)

ISU
WIRELESS
COMMUNICATION
SYSTEMS

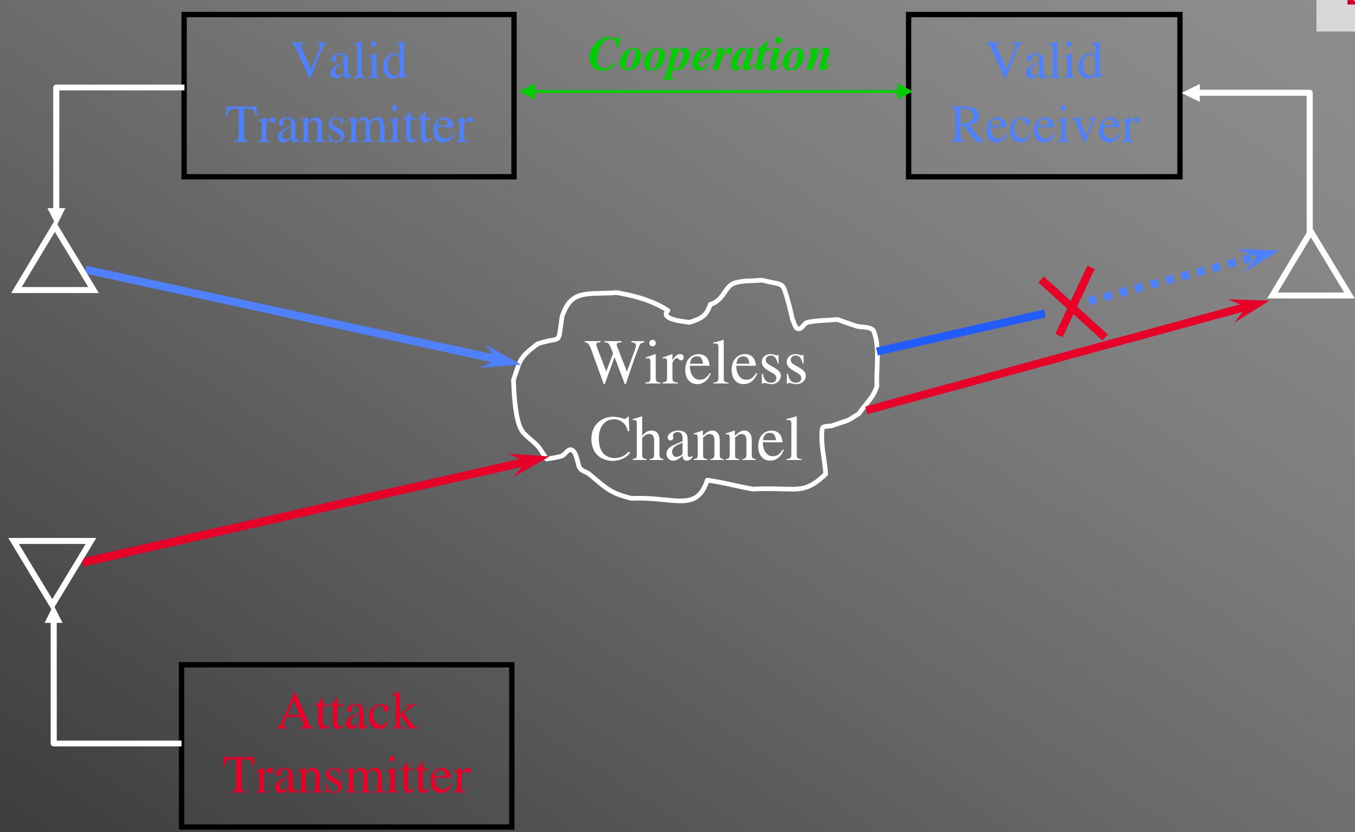


Fig. 0146

Counterfeit Base Scenario
(Spoofing Attack)

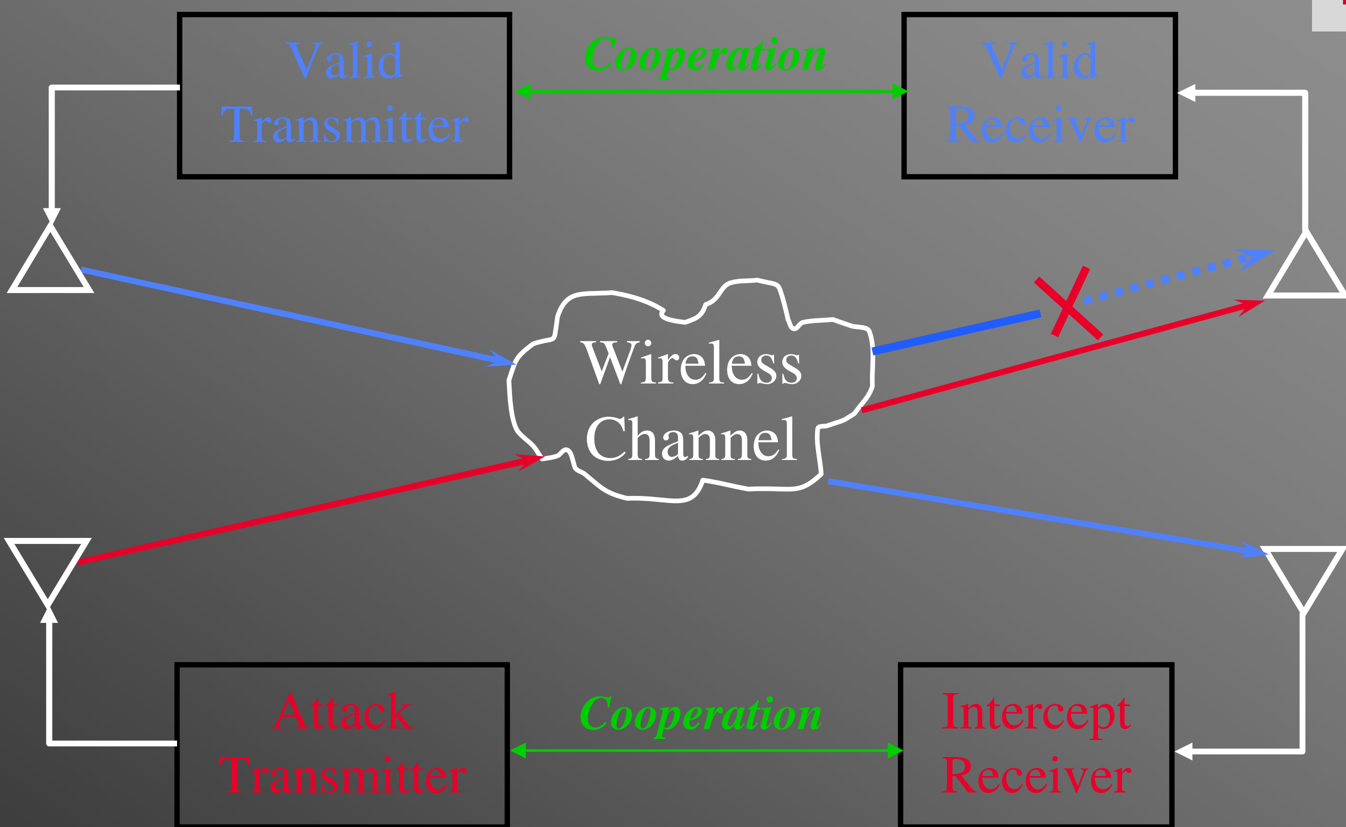


Fig. 0146

33

ISU
WIRELESS
COMMUNICATION
SYSTEMS

❖ Design Recommendations

34

Designing for Wireless Security and Reliability

ISU
WIRELESS COMMUNICATION SYSTEMS

- Adaptive (Smart) Antennas (very costly)
  - Transmitting antennas maximize EIRP in the direction of friendly receivers
  - Receiving antennas maximize directive gain in the direction of friendly transmitters
  - Receiving antennas steer a null in the direction of an interfering transmitter

Designing for Wireless Security and Reliability (cont.)

ISU
WIRELESS COMMUNICATION SYSTEMS

- Antijam Receiver Design (moderate cost increase)
  - Use frequency hopping designs
    - Direct sequence systems are too easy to jam unless the antijam (AJ) margin is large (this means a large spreading bandwidth)
  - Hop as fact as practical
    - 400-1000 hops per second should make it difficult for most follower jammers

36

Designing for Wireless Security and Reliability (cont.)

ISU
Wireless Communication Systems

- **Antijam Receiver Design (cont.)**
  - Use high-performance narrowband filters
    - These minimize interference due to out-of-band, front end overload and spurious response
  - Implement adaptive, interference-rejection spectral filters
  - Employ high-dynamic-range circuits and software algorithms
    - This minimizes overload due to high interfering signals

Designing for Wireless Security and Reliability (cont.)

ISU
WIRELESS
COMMUNICATION
SYSTEMS

CONTINUE HERE NEXT TIME

- **Antijam Receiver Design (cont.)**
  - **Implement a hopping RF preselector filter**
    - **This gives best performance but is costly**

Designing for Wireless Security and Reliability (cont.)

ISU
WIRELESS
COMMUNICATION
SYSTEMS

- Data Link (MAC) and physical layer designs
  - Design for a high error rate
  - Smaller data packets
  - Error detection <u>and correction</u>
  - Robust ACK/NAK for uncorrectable errors
  - Use data interleaving to mitigate unsophisticated jammers
    - This will probably make voice over data impractical

Designing for Wireless Security and Reliability (cont.)

ISU
WIRELESS COMMUNICATION SYSTEMS

- **Intrusion Detection and Wireless Channel Management**
  - **Much research is still needed**
  - **Monitor spectrum for interfering signals**
  - **Log historical error rates and signal levels**
    - **Alert system manager to unusual conditions**

40

Designing for Wireless Security and Reliability (cont.)

WIRELESS COMMUNICATION SYSTEMS

- Identification and Authentication
  - Both mobile and base should identify and authenticate each other
- Data Encryption at the Physical Layer
  - !DO IT!

41

Variable Levels of Service

ISU
WIRELESS
COMMUNICATION
SYSTEMS

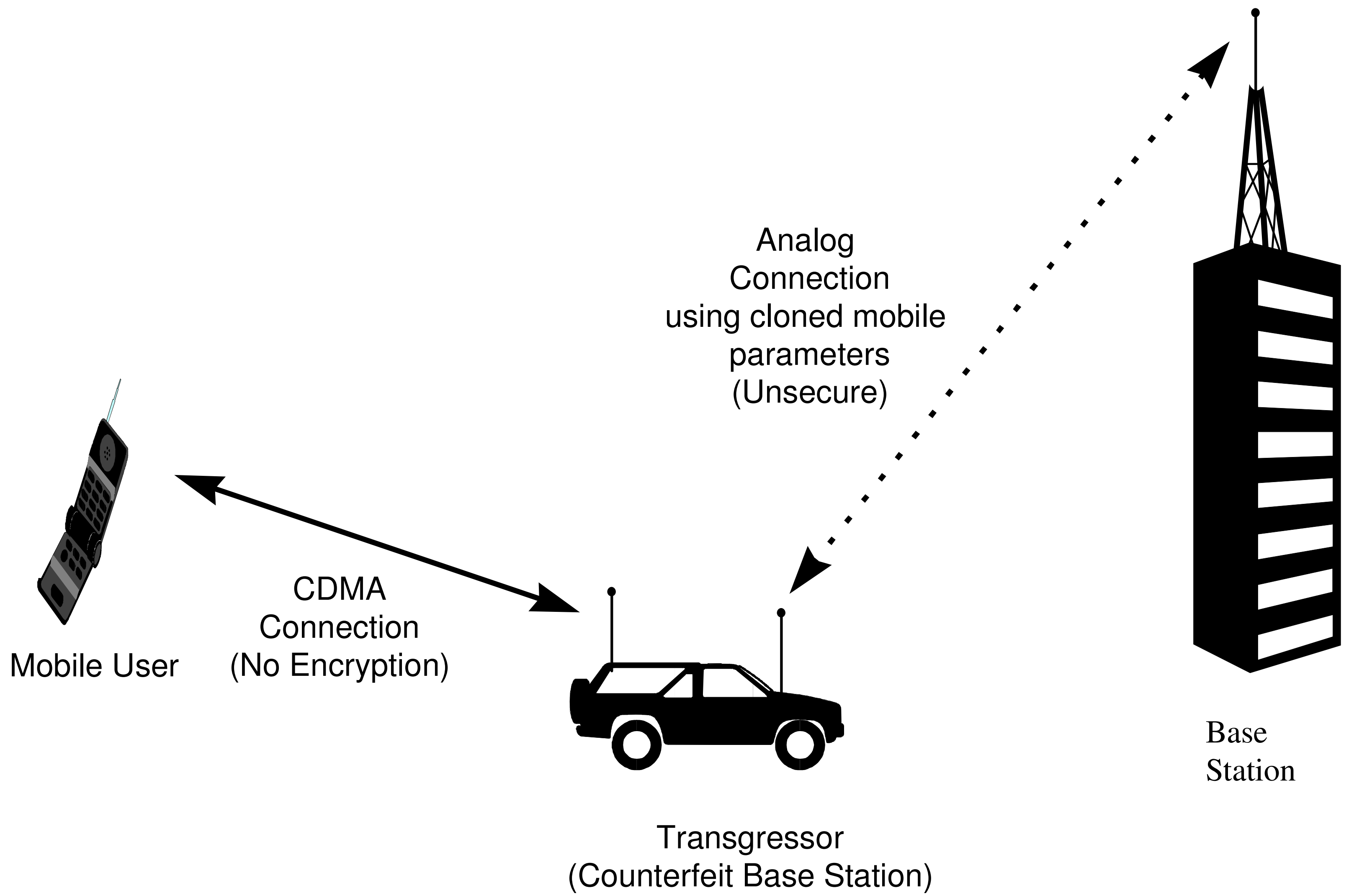
- High data rates when the RF environment is benign
- Adaptive data rates when the RF environment is hostile
- Level of service can be user selected via software or selected by automated intrusion detection

Proprietary vs. Standards

ISU
WIRELESS
COMMUNICATION
SYSTEMS

- Proprietary Systems
  - Waveform information must be gathered by signal monitoring and analysis -- sometimes a difficult and expensive task
- Standard System 802.11
  - Waveform information is readily available in the standards documents

- **Example:**
  - **IS-95 counterfeit base**



Analog
Connection
using cloned mobile
parameters
(Unsecure)
CDMA
Connection
(No Encryption)
Mobile User
Transgressor
(Counterfeit Base Station)
Base
Station

Example:
"Spectrum24(R)" System (IEEE 802.11)

WIRELESS COMMUNICATION SYSTEMS

- Operates under FCC Rules, Section 15.247
- Frequency Span of 2.4 GHz band (USA)
  - ~2400 - 2483.5 MHz
- Frequency Spreading Method
  - Frequency Hopping
- Hopping Channel Frequency Separation
  - ~1 MHz (based on 2-4 GFSK)

46

Example (cont.):
"Spectrum24(R)" System (IEEE 802.11)

WIRELESS COMMUNICATION SYSTEMS

- Number of Hopping Frequencies
  - 78 in the USA
- Hopping Dwell Time
  - 0.1 Seconds (10 hops/second)
- Modulation Format
  - Gaussian 2-4 Frequency Shift Keying (GFSK)

Example (cont.):
"Spectrum24$^{(R)}$" System (IEEE 802.11)

ISU
Wireless Communication Systems

- Data Rate
  - 1.0-2.0 Megabits per second (specifications quote both)
- Multiple Access
  - Carrier-sense, multiple access, collision avoidance (CSMA/CA)
- Power outputs
  - 500 milliwatts out of the transmitter

Example (cont.):
"Spectrum24(R)" System (IEEE 802.11)

WIRELESS COMMUNICATION SYSTEMS

- Media Access Control (MAC) layer Security
  - Not available

WIRELESS
COMMUNICATION
SYSTEMS

❖ Some Current Resources

50

Conferences and Web Sites

WIRELESS
COMMUNICATION
SYSTEMS

- Journal of Electronic Defense
  - http://www.jedefense.com
- Iowa State University - Information Systems Security Laboratory (ISSL)
  - http://www.issl.org
- Purdue University - Center for Education and Research in Information Assurance and Security
  - Http://cerias@purdue.edu
- Telecommunications and Information Security Workshop 2000 (TISW2000)
  - Tulsa, OK, Sept. 27-28, with a post-session on Sept. 29
  - http://ww.cis.utulsa.edu/tisw2000

Cellular Intercept

WIRELESS
COMMUNICATION
SYSTEMS

- FP - ELECTRONIC - Security Systems - *Swift Cellular Intercept System*
  - http://www.fp-electronic.de/swift.htm
- BARTEC, Bartlett Technologies - Communications Assistance for Law Enforcement Act (CALEA)
  - http://www.bartec.com/
  - http://www.bartec.com/content/whatshotCOPS.html
- GSM INTERCEPT WORKSHOPS
  - http://spyzone.com/spyzone/news/gsmwork.html

52

Wireless Security and Reliability

WIRELESS COMMUNICATION SYSTEMS

- QUESTIONS?

Steve F. Russell
sfr@iastate.edu

53